PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Acquisition Service DC

On-Site Electronic Contract Management System (eCMS) Support

Date: 8/25/11

Contents

1.0 BACKGROUND 3
2.0 APPLICABLE DOCUMENTS 3
3.0 SCOPE OF WORK 4
4.0 PERFORMANCE DETAILS 4
4.1 PERFORMANCE PERIOD 4
4.2 PLACE OF PERFORMANCE 5
4.3 TRAVEL 5
5.0 SPECIFIC TASKS AND DELIVERABLES 5
5.1 Contractng Support 5
5.1.1 Desk-side support: 5
5.1.2 Work with CAI-DC Supervisors: 6
5.1.3 CAI-DC Staff 6
5.1.4 Reporting FPDS-NG 6
5.1.5 Posting of Solicitation 6
5.1(a) Weekly Status report 6
5.2 Automated System administration 6
5.3 Training and User Support 7
5.3.1 Training 7
5.3.2 Individual training 7
5.3.3 Mentor 7
5.3.4 Generation of Report 7
5.3.5 Meeting Participation 7
5.3.6 Additional Assistance 7
5.4 Application Administration 8
5.4.1 Support/Application Administration 8
5.4.2 Collection of Data 8
5.4.3 Analyze and Implement report 9
5.4.4 Data Extraction from eCMS 9
6.0 GENERAL REQUIREMENTS 9
6.1 Contracting Officer Technical Representative (COTR) 9
6.2 Non-Disclosure Agreements: 9
6.3 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 9
6.4 METHOD AND DISTRIBUTION OF DELIVERABLES 11
6.5 PERFORMANCE METRICS 12
6.5.1 Invoices 12
6.5.2 Support eCMS: 12
6.6 FACILITY/RESOURCE PROVISIONS 13
6.7 GOVERNMENT FURNISHED PROPERTY 14
ADDENDUM A 15
ADDENDUM B 20

1.0 BACKGROUND

The Department of Veterans Affairs (VA) Office of Acquisition Logistics and Construction (OAL&C), Acquisition Service DC, office's primary mission is to provide contracting support to VA Central Office and the entire VA enterprise. Previously all solicitations, synopsis, and reporting actions were conducted through a manual process utilizing templates and systems outside of VA in lieu of utilizing the VA's Electronic Contract Management System (eCMS). Effective June 15, 2007, the use of eCMS became a mandatory requirement for all acquisitions over $25,000.00. Based on the mandatory requirement for the use of eCMS, Acquisition Service DC has an immediate need for eCMS support services to help the Acquisition Service DC workforce in the use of eCMS.

2.0 APPLICABLE DOCUMENTS

Documents referenced or germane to this Performance Work Statement (PWS) are listed below. In the performance of the tasks associated with this Performance Work Statement, the contractor shall comply with the following:

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
8. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” September 10, 2004
9. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
15. Homeland Security Presidential Directive (12) (HSPD-12)
16. VA Directive 6500, “Information Security Program,” August 4, 2006
17. VA Handbook 6500, “Information Security Program,” September 18, 2007
18. VA Handbook 6500.1, “Electronic Media Sanitization,” November 3, 2008.

19. VA Handbook 6500.2, “Management of Security and Privacy Incidents,” June 17, 2008.
20. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
21. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010
23. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
24. OI&T ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
25. Technical Reference Model (TRM) (reference at http://www.ea.oit.va.gov/Technology.asp)
26. National Institute Standards and Technology (NIST) Special Publications
27. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
28. VA Directive 6300, Records and Information Management, February 26, 2009
29. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

3.0 SCOPE OF WORK

The contractor shall provide on-site eCMS support to the Acquisition Service DC offices. The contractor shall provide resources that are fully trained and have the level of experience to accomplish the requirements of this PWS. The eCMS support services are required for a broad range of eCMS actions and will include training and user support, application administration, standard operating procedures, and management and reporting. In addition, the contractor personnel shall be acceptable to the Government in terms of personal and professional conduct, and in technical knowledge. Should any contractor personnel be determined to be unacceptable in terms of technical competency or unacceptable personal conduct during duty hours, the contractor shall immediately remove and replace the unacceptable on-site personnel at no additional costs to the Government. Contractor personnel shall not be put in a decision-making position during performance.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be a 12 month base period from date of award, plus one, twelve month option year. Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO**) (**If required, the CO may designate the contractor to work during holidays and weekends).

There are ten Federal holidays set by law (USC Title 5 Section 6103) that the VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities located at 1776 I Street NW, Washington, DC 20006. Work may be performed at remote locations with prior approval of the Contracting Officer Technical Representative (COTR).

4.3 TRAVEL

The Government does not anticipate there will be any travel required.

5.0 SPECIFIC TASKS AND DELIVERABLES

The contractor is responsible for providing the deliverables identified by the Acquisition Service DC contracting staff. Because much of the work to be performed is sporadic or on an "as required" basis, specific due dates for most work cannot be established until the work is actually required. All information acquired and documents developed during this contract belong to the VA.

5.1 CONTRACTING SUPPORT

5.1.1 **Desk-side support:**

The contractor shall provide desk-side support for all Acquisition Service DC eCMS users, assisting users on an ad hoc basis. Support staff shall provide telephone, e-mail, and web cast support to users.

5.1.2 **Work with Acquisition Service DC Supervisors:**

The contractor shall work with the Acquisition Service DC supervisory and user staff in support of the Gatekeeper capacity. The contractor shall support the 2237 retrieval from IFCAP into eCMS, contracting documentation validation, and workload assignments.

5.1.3 **Acquisition Service DC Staff**

The contractor shall provide support to Acquisition Service DC staff in the following areas: contract administration tasks, to help users create and manage actions/documents in eCMS Production Environment. If this is the case, separation of this effort from the core eCMS development effort will be enforced, to ensure the integrity of the limited access rules for procurement integrity.

5.1.4 **Reporting FPDS-NG**

The contractor shall provide support to users reporting of contracting actions to FPDS-NG, validation of FPDS-NG data, and completion of the validation process.

5.1.5 **Posting of Solicitation**

The contractor shall provide support to reporting, solicitation, and solicitation amendment actions to external sites (i.e. FedBizOpps and eBuy), including verifying solicitation data and documents are properly loaded and users follow proper upload procedures. The contractor shall support Solicitation Evaluation module and use of the Vendor Portal.

Deliverables:

5.1(a) **Weekly Status report**

The contractor shall provide a weekly status report detailing the tasks performed during the reporting period, and also report action items to be performed by the contractor. The report shall be submitted to the COTR in word format. This report includes all actions performed by the contractor during the performance period. Some of the reports that will be generated are: support to staff, special reports, and data extracted. This deliverable pertains to Sections 5.1.1 through 5.1.5.

5.2 Automated System Administration

The contractor shall gather and report any issues with the automated Acquisition Management System (AAMS) knowledge base (KB). Issues may include problems with Federal Acquisition Regulation (FAR) or Veterans Affairs Acquisition Regulation (VAAR) clause inclusion or exclusion in contracting documents, data values, data value descriptions and defaults, document generation problems, and any of several other types of problems that can be resolved through KB configuration. Such issues shall be reported by the contractor to the VA eCMS application administrators, and also to Aquilent, for recording as change requests (CRs).

Deliverables:

5.2(a) **Summary of issues:**

The contractor shall maintain a daily summary of any issues either discovered or reported, and provide to the COTR on a monthly basis, no later than the fifth workday of the month.

5.2(b) **Report:**
The contractor shall provide adhoc reports as requested.

5.3 Training and User Support

5.3.1 Training

The contractor shall provide ad hoc training. Such sessions will be coordinated directly with Acquisition Service DC supervisory staff and the COTR.

5.3.2 Individual training

The contractor shall provide individual, desk-side and/or classroom training to users. The training requirement may be for either 5-day eCMS End User Training sessions for new users as requested. In addition, because of new or changing contracting staff, there is an ongoing need for training new eCMS users. Typically, new staff will participate in end user training sessions. But, if participation in such training is necessary for only one or two users where a full 5-day session is not appropriate, contractor's on-site support staff will provide this training to new users. VA anticipates the number of participants in such training sessions will be very small, and that it will be possible to accelerate the end user training from 5 days to as few as 2 to 3 days.

5.3.3 Mentor

The contractor shall mentor site coordinators demonstrating how to properly use eCMS, and provide knowledge transfers so they may act as subject matter experts and administer eCMS.

5.3.4 Generation of Report

The contractor shall generate reports as requested by Acquisition Service DC staff, using the Data Warehouse.

5.3.5 Meeting Participation

The contractor shall meet with users on a regular basis monthly and gather feedback on use of eCMS, problems with the system, and ideas for enhancements.

5.3.6 Additional Assistance

The contractor shall support users in the utilization of acquisition reporting tools. Where directed by management staff, the contractor shall generate acquisition reports using available tools or, when existing tools are not adequate, by generating ad hoc reports by other means.

***Deliverables**:*

5.3.6(a) ***Training classes:***

The contractor shall provide 5 day training session for new eCMS users as required in accordance with Section 5.3.2 of this PWS. The contractor shall be responsible for reviewing and understanding the changes and the material to provide user training. Note: All training material will be provided, updated, and kept current by the eCMS software contractor to reflect the current status of the system.

5.3.6(b) ***Refresher training:***

The contractor shall provide one to two days refresher training on an as-required basis for users that have completed the 5 day new eCMS user training.

5.3.6(c) ***Reports:***

The contractor shall provide Workload and Data gathering reports generated from the MicroStrategy tool as required by Acquisition Service DC supervisory staff and the COTR.

5.4 APPLICATION ADMINISTRATION

5.4.1 Support/Application Administration

The contractor shall support application administration of the Acquisition Service DC site and user accounts, including configuration of user accounts, assignment of roles and permissions, specification of site data, identity register information, standard address data, and desktop access. This work will be in support of the eCMS system administrators, who will be the primary personnel performing these functions.

5.4.2 Collection of Data

The contractor shall collect any Acquisition Service DC contracting data artifacts and materials that may potentially be suitable for reuse by other VA contracting users, and providing those artifacts to the VA eCMS staff for review and possible posting on the Acquisition Resource Center (ARC).

Deliverables*:*

5.4.2(a) ***Day to day maintenance/troubleshooting as necessary.***

The contractor shall provide troubleshooting support to individual user who may have access issues, role issues, access to individual action, transfer actions from users, etc. The contractor shall submit change requests when appropriate (change requests resulting from issues eCMS Modules changes).

5.4.3 **Analyze and Implement report**

Analyze, design, and implement reports as requested by Office of Acquisition, Operation management staff, using acquisition data extracted from eCMS.

5.4.4 **Data Extraction from eCMS**

Support VA's requirements for extracting of information from eCMS and creation of queries and reports in Excel, Microsoft Access, or c tier tools.

6.0 GENERAL REQUIREMENTS

6.1 CONTRACTING OFFICER TECHNICAL REPRESENTATIVE (COTR)

The Contracting Officer's Technical Representative (COTR) for the task order action is:
Daniel Centeno
Acquisition Business Service1776 I Street
Washington, DC 20006
Phone: 202-756-1418
E-Mail: Daniel.Centeno@va.gov

6.2 NON-DISCLOSURE AGREEMENTS:

Non-Disclosure Agreements: The contractor's on-site representative(s) will have access to sensitive verbal, written and electronic information while performing on this task order. This information may be acquisition sensitive information, for official use only documents, or other contractor's proprietary information. In order to protect this information from unauthorized release or use, the contractor will provide an executed non-disclosure agreement to the COTR prior for the assigned on-site representative.

6.3 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The following security requirement must be addressed regarding contractor supplied equipment: contractor supplied equipment; PCs of all types, equipment with hard drives, etc. for task order services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within the VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COTR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

1. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

☒ Low/NACI
☐ Moderate/MBI
☐ High/BI

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, “”Personnel Security Suitability Program,” Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate	**Minimum Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

Contractor Responsibilities:

a. The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language. .

b. The contractor shall bear the expense of obtaining background investigations.

c. For a Low Risk designation the following forms are required: 1.OF-306 and either 2. DVA Memorandum – Electronic Fingerprints or FD-258 Fingerprint card. For Moderate or High Risk the following forms are required: 1. VA

Form 0710 and either 2. DVA Memorandum – Electronic Fingerprints or FD-258 Fingerprint card. These should be submitted to the CO or COTR after award has been made.

d. The contractor personnel will receive an email notification from the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85 or SF85P). The contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).

e. The contractor is to sign the signature page and send to the COTR and CO for electronic submission to the Security and Investigations Center (SIC).

f. The contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor shall be responsible for all resources necessary to remedy the incident.

g. If the background investigation is not completed prior to the start date of the contract, the contractor employee may work on the contract once the investigation has been initiated and sent to the OPM. However, the contractor will be responsible for the actions of the contractor personnel they provide to perform work for the VA. The investigative history for contractor personnel working under this contract must be maintained in the databases of either the OPM or the Defense Industrial Security Clearance Organization (DISCO).

h. The contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration in working under the contract.

i. Failure to comply with the contractor personnel investigative requirements may result in termination of the contract for default.

6.4 METHOD AND DISTRIBUTION OF DELIVERABLES

The contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007, MS Excel 2000/2003/2007, MS PowerPoint 2000/2003/2007, MS Project 2000/2003/2007, MS Access 2000/2003/2007, MS Visio 2000/2002/2003/2007, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.5 PERFORMANCE METRICS

The Government will evaluate contractor performance and deliverables against the critical performance objectives provided in the tables below to determine if the services rendered are acceptable for payment. Payment will be made on a monthly basis as identified in the Contract Line Item Number (CLIN) in the Schedule.

6.5.1 **Invoices**

Services will be accepted on a monthly basis by certification of the monthly invoice. All required deliverables and performance objectives must be fulfilled in order to obtain acceptance. Acceptance will constitute 100% payment. Non-acceptance may result in negotiation of a credit commensurate with the negative impact on the Acquisition Service DC mission resulting from the reduced level of performance. Said credit will be negotiated at the time of non-acceptance. Failure to agree on a credit amount will be considered a dispute in accordance with the Disputes Clause of the contract action. To assure quality standards are met, service provider shall meet with the COTR, or designee, on a bimonthly basis.

6.5.2 **Support eCMS:**

Performance Objective	**Performance Standard**	**Monitoring Method**
Contracting Support	a. Provide desk-side support for all Acquisition Service DC eCMS users, assisting users on an ad hoc basis. Support staff will provide telephone, e-mail, and web cast to users 100% of the time. b. Work with the Acquisition Service DC supervisory and super user Gatekeeper capacity. Will assist with retrieval of 2237s from IFCAP into eCMS, validate contracting documentation, and assist with workload assignments 100% of the time. c. Provide support to Acquisition Service DC staff with contract administration tasks, to help users create and manage actions/documents n eCMS 100% of the time. FPDS-NG data and completion of the validation process 100% of the time. e. Provide support to users with reporting of solicitation and solicitation amendment actions to FedBizOpps, including verifying solicitation data and documents are properly loaded into FedBizOpps and those users follow proper FedBizOpps upload procedures 100% of the time. f. Provide support to users with communication of solicitation and solicitation amendment actions to GSA's e-Buy system, utilizing e-Buy Connect 100% of the time. g. Provide support to users in adoption and use of the Solicitation 100% of the time. h. Gather and report any issues with the AAMS knowledge base (KB) and report such issues to the VA eCMS application administrators for recording as change requests (CRs) 100% of the time.	COTR review of complaints and observance of performance
Training and User support.	a. Coordinate and provide ad hoc training 100% of the time. Such training sessions shall be coordinated directly with Acquisition Service DC supervisory staff and the eCMS COTR. b. Conduct eCMS End User Training sessions. c. Mentor site coordinators in proper use of eCMS and administer eCMS 100% of the time. d. Utilize the Data Warehouse generation of reports, as requested by Acquisition Service DC staff 100% of the time. e. Meet with users at least monthly and gather feedback on use of eCMS, problems with the system, and ideas for enhancements 100% of the time.	COTR review of complaints and observance of performance.

Application Administration	a. Support application administration of the Acquisition Service DC site and user accounts, including configuration of uses accounts, assignment of roles and permissions, specification of site data, identify by register information, standard address data, and desktop access 100% of the time. This work will be in support of the eCMS system administrators, who will be the primary personnel performing these functions. b. Collect any Acquisition Service DC contrasting data artifacts and materials that may potentially be suitable for reuse by other VA contracting users, and providing those artifacts to the VA eCMS staff for review and possible posting on the Acquisition Resources Center (ARC) 100% of the time.	COTR review of complaints and observance of performance.
Standard Operating Procedures (SOPs)	a. Identify any modifications or additions that may need to be made to the SOPs, make those changes, validate the changes with Acquisition Service DC staff, and re-distribute the SOPs to the contracting staff 100% of the time. b. Provide support to Acquisition Service DC and other relevant users in creation of new milestone plans, or in modification of existing milestone plans 100% of the time.	COTR review of complaints and observance of performance.
Measurement and Reporting	a. Provide a weekly status report concerning this effort, and also report action items. This status report will b.: separate from the weekly eCMS status report, but the status will be discussed during the weekly project status meetings. 100% of the time. b. Analyze, design, and implement reports as requested by Acquisition Service DC management staff, using acquisition data extracted from eCMS 100% of the time. c. Support VA's requirements from extraction of information from eCMS and creation of queries and reports in Excel, Microsoft Access, or other tools 100% of the time.	COTR review of complaints and observance of performance
Comply with all applicable VA security and non-disclosure agreement requirements.	No reportable security violations and no instances of unauthorized release of sensitive information (either VA internal information or contractor business sensitive information) during the rating period.	COTR review of' complaints and observance of performance.
Effective Communication	No less than 3 contacts per week from contractor, 100% of the time	COTR review of' complaints and observance of performance.
Network Availability	Maintain Network Availability 24/7, 95% Availability, measured on a monthly basis	COTR review of' complaints and observance of performance.
Response to VA Query	Responses received within 4 business hours of request, 95% of the time measured on a monthly basis	COTR review of' complaints and observance of performance.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.6 FACILITY/RESOURCE PROVISIONS

The Government shall provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the contractor has contact. The contractor shall consider the COTR as the final source for needed Government documentation when the contractor fails to secure the documents by other

means. The contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

The VA shall provide access to VA specific systems/network as required for execution of the task via a site-to-site VPN or other technology, including VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The contractor shall not transmit, store or otherwise maintain sensitive data or products in contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

6.7 GOVERNMENT FURNISHED PROPERTY

Not Applicable

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.[1] The contractor's firewall and web server shall meet or exceed the VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Each documented initiative under this contract incorporates the security clause VAAR 852.273-75 by reference as though fully set forth therein, as well as the VA Handbook 6500.6, "Contract Security," March 12, 2010, in its entirety. Both the security clause VAAR 852.273-75 and the VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The contractor shall complete all mandatory training courses identified on the current external VA training site, the Employee Education System (EES), and will be tracked therein. The EES may be accessed at https://www.ees-learning.net/librix/loginhtml.asp?v=librix. If the decision is made by the local Program Office to provide the contractor an LMS account, the contractor shall use the VA Learning Management System (LMS) to complete their mandatory training, accessed at https://www.lms.va.gov/plateau/user/login.jsp.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). The VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards:

[1] See VAAR 852.273-75 referenced *infra*.

The contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http//www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems

_x_ § 1194.22 Web-based intranet and internet information and applications

_x_ § 1194.23 Telecommunications products

_x_ § 1194.24 Video and multimedia products

_x_ § 1194.25 Self contained, closed products

_x_ § 1194.26 Desktop and portable computers

_x_ § 1194.31 Functional Performance Criteria

_x_ § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The contractor and their personnel shall wear visible identification at all times while they are on the premises.

2. VA does not provide parking spaces at the work site; the contractor must obtain parking at the work site if needed. It is the responsibility of the contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the contractor under any conditions.

3. Smoking is prohibited inside/outside any building other than the designated smoking areas.

4. Possession of weapons is prohibited.

5. The contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a contractor or vendor in accordance with the requirements document. The contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and

164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The contractor will have access to some privileged and confidential materials of the VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The contractor shall release no information. Any request for information relating to this contract presented to the contractor shall be submitted to the VA Contracting Officer for response.

3. Contractor personnel recognize that in the performance of this effort, contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.

4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this task order on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

6. Contractor shall maintain physical security at all facilities housing the activities performed under this task order, including any contractor facilities according to VA-approved guidelines and directives. The contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy

and confidentiality of such information as required by the VA.

7. Contractor must adhere to the following:

    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any contractor (or subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/contractor relationships.

ADDENDUM B

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

B1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

1. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

2. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

4. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of

communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

5. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

4. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA

information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

11. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle

cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.

2. The contractor/subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system

development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The contractor/subcontractor agrees to:

    a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

        i. The Systems of Records (SOR); and

        ii. The design, development, or operation work that the contractor/subcontractor is to perform;

    b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

    c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.

    a. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within their contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully

responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

3. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

4. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the

system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

5. The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The Government reserves the right to conduct such an assessment using Government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

6. VA prohibits the installation and use of personally-owned or contractor/subcontractor owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a task order, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

8. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

    a. Vendor must accept the system without the drive;

b. VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

c. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

d. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

i. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

ii. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

iii. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

1. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

2. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information.

Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

4. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

2. The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

3. Each risk analysis shall address all relevant information concerning the data breach, including the following:

    a. Nature of the event (loss, theft, unauthorized access);

    b. Description of the event, including:

        i. date of occurrence;

ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

c. Number of individuals affected or potentially affected;

d. Names of individuals or groups affected or potentially affected;

e. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

f. Amount of time the data has been out of VA control;

g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

h. Known misuses of data containing sensitive personal information, if any;

i. Assessment of the potential harm to the affected individuals;

j. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

k. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

4. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

a. Notification;

b. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

c. Data breach analysis;

d. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

e. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

f. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

1. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

    a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;

    b. Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;

    c. Successfully complete *VHA Privacy Policy Training* if contractor will have access to PHI;

    d. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

    e. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

2. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the task order until such time as the training and documents are complete.

Exhibit 1

CONTRACTOR RULES OF BEHAVIOR

This User Agreement contains rights and authorizations regarding my access to and use of any information assets or resources associated with my performance of services under the task order terms with the Department of Veterans Affairs (VA). This User Agreement covers my access to all VA data whether electronic or hard copy ("Data"), VA information systems and resources ("Systems"), and VA sites ("Sites"). This User Agreement incorporates Rules of Behavior for using VA, and other information systems and resources under the task order.

GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS AND ACTIVITIES UNDER THE TASK ORDER:

a. I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.
b. I consent to reviews and actions by the Office of Information & Technology (OIT) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the task order terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.
c. I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OIT, VA, and law enforcement personnel.
d. I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal Government systems; deny access to Federal Government systems; accrue resources for unauthorized use on Federal Government systems; or otherwise misuse Federal Government systems or resources are prohibited.
e. I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).
f. I agree that OIT staff, in the course of obtaining access to information or systems on my behalf for performance under the task order, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers

(ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.
g. I understand I must comply with VA's security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer's Technical Representative (COTR). If the contractor believes the policies and guidance provided by the COTR is a material unilateral change to the task order, the contractor must elevate such concerns to the Contracting Officer for resolution.
h. I will report suspected or identified information security/privacy incidents to the COTR and to the local ISO or Privacy Officer as appropriate.

GENERAL RULES OF BEHAVIOR

a. Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job.

b. The following rules apply to all VA contractors. I agree to:

(1) Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the task order.
(2) Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.
(3) I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the task order. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.
(4) Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the task order.
(5) Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the task order or at the direction of the COTR or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not confer me unrestricted access or use, nor the authority to bypass security or other controls except as expressly permitted by the VA CIO or CIO's designee.
(6) Contractors' use of systems, information, or sites is strictly limited to fulfill the terms of the task order. I understand no personal use is authorized. I will only use other Federal Government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal law still apply.

(7) Grant access to systems and information only to those who have an official need to know.
(8) Protect passwords from access by other individuals.
(9) Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.
(10) Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the task order terms with the VA.
(11) Follow VA Handbook 6500.1, *Electronic Media Sanitization* to protect VA information. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders.
(12) Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.
(13) Not host, set up, administer, or run an Internet server related to my access to and use of any information assets or resources associated with my performance of services under the task order terms with the VA unless explicitly authorized under the task order or in writing by the COTR.
(14) Protect Government property from theft, destruction, or misuse. I will follow VA directives and handbooks on handling Federal Government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the COTR.
(15) Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders regarding my access to and use of any information assets or resources associated with my performance of services under the task order terms with VA.
(16) Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated with my performance of services under the task order terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the COTR.
(17) Understand that restoration of service of any VA system is a concern of all users of the system.
(18) Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

ADDITIONAL CONDITIONS FOR USE OF NON- VA INFORMATION TECHNOLOGY RESOURCES

a. When required to complete work under the task order, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible then I will use VA approved remote access software and services.
b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.
c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.
d. I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given task order or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same.

STATEMENT ON LITIGATION

This User Agreement does not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

ACKNOWLEDGEMENT AND ACCEPTANCE

I acknowledge receipt of this User Agreement. I understand and accept all terms and conditions of this User Agreement, and I will comply with the terms and conditions of this agreement and any additional VA warning banners, directives, handbooks, notices, or directions regarding access to or use of information systems or information. The terms and conditions of this document do not supersede the terms and conditions of the signatory's employer and VA.

_____	_____
Print or type your full name	Signature
_____	_____
Last 4 digits of SSN	Date
_____	_____
Office Phone	Position Title

_____
Contractor's Company Name

Please complete and return the original signed document to the COTR within the timeframe stated in the terms of the task order.

Exhibit 2
Non-Disclosure Agreement

The following form is required to be executed and submitted by each contractor employee:

6.1 CONFIDENTIAL INFORMATION AGREEMENT

6.2 TASK ORDER/CONTRACT NO. _____

I, _____, am an /__/ employee /__/ contract employee of_____ ("contractor"). The contractor has contracted with the Department of Veterans Affairs (VA), the "Customer", to perform various contract administration support and related services. I understand and acknowledge that, as a result of my employment with contractor, I may have access to certain confidential, proprietary, and other information including, within specified parameters and only as allowed by law, access to VA's computer programs and software, processes, technical information, plans, specifications, files, directives, financial records, and, possibly, the tenants of federal buildings. Confidential information shall not include information to the extent that: (i) it is or becomes publicly available through a source other than contractor; (ii) it is required to be disclosed pursuant to law or regulation, Government authority, duly authorized subpoena or court order; (iii) is approved for disclosure by prior written consent of VA; or (iv) information that the contractor subsequently learned from a third party that does not impose an obligation of confidentiality upon contractor and that either (a) does not reference or identify VA or VA's customer client, other contractors, or any files or employees of the same; or (b) which references or identifies VA, or VA's customer client, other contractors, or any files or employees of the same, but which after reasonably inquiry cannot be determined to be Confidential Information covered by this Agreement.

6.2.1 I will not at any time, either during or after my employment or contract with the contractor, use or disclose to others or any other source outside VA, any confidential information obtained as a result of the task order between contractor and VA or as the result of any access to VA's customer client's or other contractor's files, computers or personnel.

I acknowledge I have been assigned to or I am working on the task order indicated above at the direction of VA and that any product of my work is intended to be privileged and confidential work product. I am aware that unauthorized disclosure of information could damage the integrity of this task order, or project(s), as well as other Governmental interests and that the transmission or revelation of such information to unauthorized persons could subject me to prosecution under applicable laws.

I agree that I will not divulge, publish, or reveal by work, conduct or any other means, such confidential, proprietary, and sensitive information or knowledge, except as

necessary to do so in the performance of my official duties related to this task order and Project and in accordance with the laws of the United States, unless specifically authorized in writing, in each and every case, by the task order's Project Manager, Contracting Officer, or a duly authorized representative of the United States Government. I take this obligation freely, without any mental reservation or purpose of evasion and in the absence of duress.

Upon completion of the task order, or project, I will safeguard and not disclose to any other source, customers, clients or parties, other than to VA, or properly authorized personnel of VA's customer client or of another Federal agency without limitation, any and all research findings, documents or papers relating to VA or VA's customer client's or other contractor's business in my possession, under my control or accessible by me.

I agree that I will limit reproduction and/or dissemination of covered materials, information and data only to persons/parties related to this task order or otherwise authorized to receive such information; and, I shall make every possible effort that is reasonable and prudent to prevent unauthorized disclosure of such information covered by this Confidential Information Agreement.

I recognize that if I breach this Confidential Information Agreement, harm may come to the Government, VA, to VA's customer client, or other contractor, and that the remedy at law may be inadequate; therefore, I agree VA is entitled to seek injunctive relief against any such actual or threatened breach, in addition to any other remedy provided by law.

I agree that this agreement (a) shall be binding upon my legal representatives, and assigns; and (b) shall be governed by the laws of the United States Government.

By:_____ _____

Original Signature of Employee **Date Executed**

_____ _____

Printed Name of Employee **Title of Employee**

Original Executed Agreement to be delivered to: _____, Contracting Officer